AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, Justin N. Pearse, being duly sworn, depose and state that:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to authorize law enforcement officers to complete the search, seizure, and subsequent examination of the three (3) electronic devices identified in Attachments A-1, A-2, and A-3. This search is to encompass all available data within the device, to include but not be limited to any and all text messages, third-party application communications, images, photos, live photos, screenshots, videos, web history, google searches, call records – missed, outgoing, incoming, voicemails, and application usage. This Court has authority to issue the warrant pursuant to Federal Rules of Criminal Procedure Rule 41(b)(1) & (2), as the electronic devices to be searched are currently held as evidence by investigators within the District of New Hampshire.
2. I am currently a Drug Enforcement Administration ("DEA") Task Force Officer ("TFO") with the Southern New Hampshire DEA High Intensity Drug Trafficking Area Task Force in the Manchester District Office ("MDO") and have been so assigned since November 2021. As a DEA TFO, my duties and responsibilities include the investigation of federal crimes, including violations of 21 U.S.C. §§ 841(a)(1) & 846.
3. I have been employed as a Police Officer with the Nashua, New Hampshire Police Department since December 2011. At the Nashua Police Department, I currently serve as a Detective in the Narcotics Intelligence Division, where I have been assigned since November 2019. My primary responsibility in this position is to investigate Misdemeanor and Felony-level narcotics investigations occurring within the Jurisdiction of Nashua. I graduated from the New Hampshire

Police Standards and Training Council Police Academy in August 2009. I have attended multiple drug related investigation courses. These courses include but are not limited to; Reid Interview and Interrogation, Death and Homicide, Desert Snow motor vehicle concealment certification, Desert Snow Roadside Interdiction, Operation Pipeline Roadside Interdiction certification, Top Gun Undercover Narcotics Academy, Digital Evidence certification – National Computer Forensics Institute, along with several other narcotics courses instructed by the High Intensity Drug Trafficking Area (HIDTA), Louisiana State Highway Patrol, and Drug Enforcement Administration.

4. I have investigated numerous crimes involving the possession, sale and possession with the intent to sell various controlled drugs. I have assisted in drug investigations involving various federal, local and state law enforcement agencies. The investigations targeted street level dealers to major suppliers of illegal drugs. I have participated in many cases that have resulted in arrests, search warrants, and successful prosecutions at the state and federal levels.
5. I have worked in a plain clothes capacity and have personally observed the distribution, sale and possession of various controlled substances including, but not limited to cannabis, cocaine, cocaine-based substances, fentanyl, heroin, hashish, crystal methamphetamine and various illegally manufactured and/or obtained pharmaceutical drugs.
6. Based upon my training and experience, I am familiar with drug traffickers' methods of operation, including the distribution, storage, and transportation of drugs and the collection of money that constitutes the proceeds of drug trafficking activities. I am familiar with the types of packaging used to distribute controlled substances as well as equipment used such as scales, bags, pill presses and cutting agents. I am also familiar with drug-related paraphernalia and the equipment used to ingest controlled substances, such as syringes and smoking pipes. I have

talked to drug dealers and listened to their conversations, so I am familiar with the coded language often used in these conversations. I am also familiar with the use of cell phones by drug traffickers in order to conduct their business with both customers and co-conspirators. Because of my training and experience, I am familiar with new trends of concealing illegal drug trafficking. I also stay current on the latest technology used to investigate drug crimes. In sum, through my training, education, and experience, I have become familiar generally with the manner in which drug traffickers conduct their illegal activities, including purchasing, manufacturing, storing, and distributing drugs, the laundering of illegal proceeds, and the efforts of persons involved in such activity to avoid detection by law enforcement. Observations made and conclusions drawn throughout this affidavit that are based on my training and experience also include the training and experience of other law enforcement agents and officers with whom I have discussed these issues.

7. Based upon my training and experience, I am aware that drug traffickers commonly use cellular telephones to communicate and further their drug-trafficking activities. However, drug traffickers are aware of law enforcement's use of electronic surveillance, and thus frequently endeavor to thwart detection by changing cellular telephone numbers, using multiple cellular phones at the same time, utilizing prepaid cellular phones where the user of the phone is not required to provide personal identifying information, and/or use encrypted communication applications. I am also aware that in addition to using multiple phones to thwart detection, drug traffickers commonly use multiple phones as they maintain different lines of service for customers located in separate regions/states. It is also common for those involved in the possession and sale of illicit drugs to maintain possession of previously used phones to preserve the data contained within. I am also aware that drug traffickers frequently "drop" or change

cellular telephone numbers or the physical electronic devices in an effort to thwart law enforcement's use of electronic surveillance.

8. I am familiar with the facts and circumstances of this investigation from my own personal participation and from oral and written reports given to me by New Hampshire Concord Police Department ("CPD") Detective Paul Shaughnessy.

9. Based on my training and experience, and for all the reasons set forth herein, I submit that probable cause exists to believe that the requested information in this warrant will constitute or lead to evidence of offenses involving possession with intent to distribute controlled substances, including but not limited to; crack cocaine, fentanyl and/or heroin, and Methamphetamine, in violation of 21 U.S.C. § 841(a)(1), and conspiracy to distribute controlled substances, in violation of 21 U.S.C. § 846, and use of a communication facility during or in relation to a controlled substances trafficking offense, in violation of 21 U.S.C. § 843(b) (the "Target Offenses"), as well as the identification of individuals who are engaged in the commission of the Target Offenses.

10. Since this affidavit is being submitted for the limited purpose of establishing that probable cause exists to support the issuance of this search warrant, I have not included details about every aspect of the investigation. While this affidavit contains all the material information I am aware of that is pertinent to the requested search warrant, it does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

11. The property to be searched, as described in Attachments A-1, A-2, and A-3, hereinafter referred to as the **Target Devices**, is:

    a. Black colored Samsung cellular telephone (CPD Evidence 23-1479-PR)

b. Black colored cellular telephone, believed to be a Samsung Z (CPD Evidence 23-1480-PR)
c. Blue colored Apple iPhone cellular telephone (CPD Evidence 23-1534-PR)

12. These devices are currently in law enforcement possession. The electronic devices identified in Attachments A-1, A-2, and A-3 are believed to be owned and maintained by the same individual, Noble Hunt, Date of Birth: [redacted] These electronic devices were located and seized from the same motor vehicle upon the execution of a search warrant, and it was learned through a custodial interview with Hunt that the same SIM (Subscriber Identity Module) card was shared between all of his devices.

13. The applied-for warrant would authorize the forensic examination of the **Target Devices** for the purpose of identifying electronically stored data particularly described in Attachment B-1, B-2, B-3.

PROBABLE CAUSE

14. I am currently participating in an investigation into the suspected criminal activity of Noble Hunt, along with investigators from CPD and Department of Homeland Security ("HSI"). Hunt was identified by investigators as a local poly-drug narcotics distributor operating in the greater Concord, New Hampshire area, with associations to significant poly-drug trafficking organizations operating in the Commonwealth of Massachusetts. During the initiation of this criminal investigation, Hunt was wanted on an outstanding warrant issued for his arrest as a result of narcotic offenses in the State of Maine.

15. On Friday, March 17, 2023, CPD obtained a search warrant for Noble Hunt's Facebook account. On Tuesday, March 21, 2023, Detective Shaughnessy received records from Hunt's Facebook account. Hunt's Facebook account detailed Hunt's involvement and the distribution of significant quantities of illicit drugs. Of note, Hunt conversed with an individual named,

"Francis Andujar," who appeared to be Hunt's primary source of supply. In one series of messages, "Francis" asked Hunt for $12,000 in cash, and in turn would give Hunt three hundred grams of pure "feta." The term, "feta," is believed to be slang for the controlled drug, fentanyl. "Francis" further told Hunt that he was going to give Hunt, "1 lb of ice." Based on my training, and prior drug investigations, "ice" is a street-level term used to describe the illicit drug, Methamphetamine.

16. Furthermore, there were communications between Hunt and "Matthew James." During the course of this investigation, CPD learned that "Matthew James" was an alias used by Matthew Hansen on Facebook. Through these Facebook communications between Hunt and Hansen, it appeared that Hunt had recently sold drugs to Hansen.

17. On Wednesday, March 22, 2023, CPD responded to [redacted] in Concord, New Hampshire for the report of a male overdosing in a black Volkswagen sedan bearing New Hampshire registration 3312750. This vehicle was registered to, Michael Masiello, who was known to investigators for a previous call for service. Additionally, it was known that Hunt had previous associations with this vehicle based on Facebook Messenger conversations with Masiello.

18. In my training and experience, I know that individuals can access and send messages through Facebook and Facebook Messenger using an app on a cellphone, tablet, or other electronic device.

19. CPD investigators responded to the area and located the aforementioned vehicle parked in the back corner of the parking lot. An investigator observed a male slumped forward in the driver's seat of the vehicle. Upon the investigator's approach, the male appeared to awaken. The vehicle was still running, and the investigator saw a smoking pipe sticking out from between the male's legs. The investigator asked the male for his driver's license. The male provided him with a

New Hampshire Driver's License and identified himself as Ryan Garrison, Date of Birth: [redacted] The investigator asked the male to step out of the vehicle, and noticed that as he did so, the male attempted to conceal the smoking pipe along with a glassine bag containing a white rock-like substance. The investigator believed the aforementioned substance to be an illicit drug; however, the male denied there were any drugs in the car.

20. Under the belief that this male was providing a false identity and while still investigating the facts of the suspected overdose, additional investigators responded to [redacted] to assist. An investigator observed the male, who identified himself as Garrison, as Noble Hunt. An investigator secured Hunt in handcuffs and told him he was being detained. Hunt would not formally identify himself on scene. Hunt was ultimately taken into custody and transported to CPD where he was formally identified through the booking process, and with the assistance of the Automated Fingerprint Identification System.

21. While remaining on scene, an investigator observed within the Volkswagen's driver's side door and without moving or manipulating the door or its contents, what he believed to be a large quantity of pressed Heroin/Fentanyl in plain-view. Given this observation, the vehicle was seized pending the application of a search warrant.

22. On Friday, March 24, 2023, CPD executed the search warrant on the Volkswagen sedan. This search revealed a large quantity of separately packaged narcotic drugs along with evidence of drug sales within the vehicle. This included approximately 983 grams of Fentanyl, 209 grams of Cocaine, 175 grams of Crack Cocaine, and 110 grams of Methamphetamine. Additionally, $17,140.00 in bulk United States currency, a drug ledger, a commercial drone, and the **Target Devices**.

23. On Wednesday, March 29, 2023, investigators responded to the Merrimack County Department of Corrections where Hunt was arrested for four counts of Possession of a Controlled Drug with the Intent to Distribute.

24. Hunt knowingly and voluntarily waived his *Miranda* Rights and agreed to speak to investigators. During this interview, Hunt acknowledged his involvement in the possession and sale of illicit drugs. Hunt identified the contents of the vehicle as belonging to him. Hunt indicated that he used three to four cell phones and that the same subscriber identity module card, or SIM card, was recycled between them. Hunt said that currently, the SIM card was likely housed within the Samsung S22 Ultra and was positioned closest to him in the motor vehicle. Hunt also identified the commercial drone as belonging to him, indicating that he utilized the drone to make drug deliveries to prospective customers, conduct surveillance, and identify and follow local law enforcement.

USE OF CELLULAR PHONES TO FACILITATE CRIMINAL ACTIVITY

25. Based upon training, knowledge, and experience as well as from information obtained from other law enforcement officers, I know that it is common practice for individuals engaged in criminal activity to routinely utilize cellular phones, text messaging applications, social media, and coded communications to interact with and do business with co-conspirators. Further, I know that individuals engaged in criminal activity often use cellular phones to plan and facilitate criminal activity. Therefore, I know that evidence of the crimes listed above can be found in cellular phones similar to the **Target Devices**. Such evidence includes, but is not limited to:

    a. Names, addresses, telephone numbers, usernames, and email addresses of co-conspirators;

b. Messages/emails sent to or received from co-conspirators or other entities necessary for conducting illegal activity such as arranging travel and transportation;

c. Photographs/videos of themselves and co-conspirators;

d. Photographs/videos of contraband and proceeds of illegal activity;

e. Records of social media and app usage in furtherance of illegal activity;

f. Records of internet activity in furtherance of illegal activity;

g. Calendar entries and to-do lists; and

h. Financial information and bank accounts used in furtherance of illegal activity.

TECHNICAL INFORMATION

26. Based upon my training, knowledge, and experience, I know that cellular telephones such as the **Target Devices** are capable of storing information including, but not limited to, text and audio communications, call history, contact information, calendar entries, downloads, applications, videos, photographs, and electronic documentation in the cellular telephone's memory. In addition, I know that a forensic examination of a cellular telephone and these other devices can result in the retrieval of such data which has been stored on them, even after the passage of time, because files that have been hidden or deleted can still be recovered.

27. It is also known that some mobile devices contain a Subscriber Identity Module (SIM card) that may contain data associated with the device and user attribution such as telephone number, user identity, network authorization data, and other user data commonly used by cellular telephones to identify a particular user (subscriber) to the network. This data can be recovered forensically.

28. It is also known that some mobile devices may contain removable media cards. These cards are commonly referred to as SD cards or MicroSD cards. These cards can be used to store additional data associated with the mobile device including photographic images, videos, text files and

other digital data. Additional data contained within these files may also provide dates, times, locations, settings, devices used, and user attribution information. This data can be recovered forensically.

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

    a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

    b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory

cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

30. I know that many smartphones like the **Target Devices** (which are included in Attachment B-1, B-2, and B-3's definition of "computer hardware") can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

32. *Forensic evidence*. As further described in Attachments B-1, B-2, and B-3, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **Target Devices** were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Target Devices** because:

    a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

    b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

    c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

    d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on

other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

33. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

34. *Manner of execution*. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto any premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

35. Based on the information described above, I believe that there is probable cause that the **Target Devices** contains evidence of violations of 21 U.S.C. §§ 841 & 846 (Possession with Intent to Distribute Controlled Substances, Conspiracy to Distribute Controlled Substances) and 21 U.S.C. § 843(b) (use of a communication facility during or in relation to a controlled substances trafficking offense) committed by Hunt and others. Specifically, I believe the **Target Devices** will contain messages related to drug trafficking between Hunt and others. I also believe the **Target Devices** will contain location information which could identify stash houses and other

relevant locations used by Hunt to obtain drugs. Additionally, I believe the **Target Devices** may contain information about which financial institutions are used by Hunt and other unknown co-conspirators to facilitate the distribution of controlled substances.

/s/ Justin N. Pearse
Justin N. Pearse, Task Force Officer
Drug Enforcement Administration

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

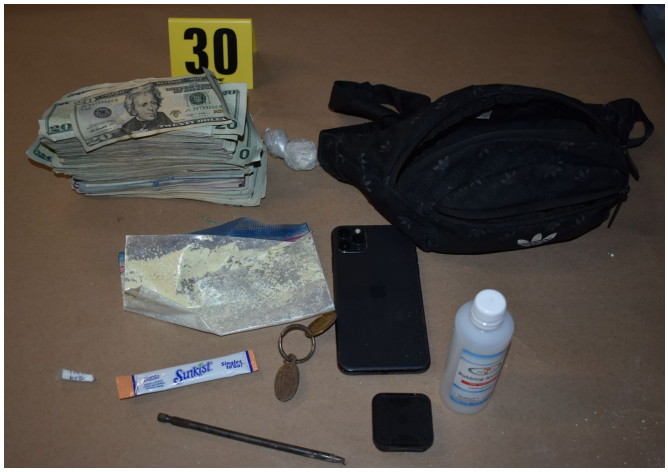
Date: Jun 12, 2023
Time: 5:00 PM, Jun 12, 2023

HONORABLE ANDREA K. JOHNSTONE
United States Magistrate Judge

ATTACHMENT A-3

Pursuant to an investigation for violations of 21 U.S.C. §§ 841 and 846, and 21 U.S.C. §843(b), this Warrant authorizes the law enforcement agents and officers to whom it is directed to a complete search, seizure, and subsequent examination of:

Blue colored Apple iPhone cellular telephone (23-1534-PR)



This warrant authorizes the forensic examination of this device for the purpose of identifying the electronically stored information described in Attachment B-3.

ATTACHMENT B-3

Description of Information or Items to Be Seized

I. All records on a Blue colored Apple iPhone cellular telephone (23-1534-PR) described in Attachment A-3, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 21 U.S.C. §§ 841 & 846 (Distribution of Controlled Substances, Conspiracy to Distribute Controlled Substances) and 21 U.S.C. § 843(b) (use of a communication facility during or in relation to a controlled substances trafficking offense) involving Hunt and other co-conspirators since March 24, 2022, including but not limited to:

A. Evidence of who used, owned, or controlled the equipment;

B. Evidence of the user's past whereabouts;

C. The identities and aliases of individuals who participated in the violations listed above;

D. Lists of associates and related identifying information;

E. Content associated with the above violations, including any information relating to types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

F. All bank records, checks, credit card bills, account information, and other financial records;

G. The locations where evidence, fruits, instrumentalities, or other items related to the violations listed above were obtained, is stored, or has been discarded;

H. The methods of communication between individuals engaged in the violations listed above, including the telephone numbers, messaging applications, and social media accounts used by the individuals;

I. The substance of communications regarding the planning, execution, transactions, and/or discussions of the violations listed above;

J. The substance of communications regarding the acquisition or disposal of items involved in the violations listed above;

K. The substance of communications regarding controlled substances, money, vehicles, communications devices, or other items acquired during or for activity that would result in the violations listed above;

L. Photographs of items or information related to the violations listed above;

M. The relationship between the users of the equipment and other co-conspirators;

N. The identity, location, and travel of users of the **Blue colored Apple iPhone cellular telephone (23-1534-PR)** and any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the violations listed above;

O. Evidence of malicious computer software that would allow others to control the equipment, software, or storage media, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;

P. Evidence of the attachment of other hardware or storage media;

Q. Evidence of counter-forensic programs and associated data that are designed to eliminate data;

R. Passwords, encryption keys, and other access devices that may be necessary to access the equipment;

S. Records relating to accounts held with companies providing Internet access or remote storage of either data or storage media; and

II. Evidence of user attribution showing who used or owned the **Blue colored Apple iPhone cellular telephone (23-1534-PR)** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

III. Serial numbers and any electronic identifiers that serve to identify the equipment.

DEFINITIONS

For the purpose of this warrant:

A. "Equipment" means any hardware, software, storage media, and data.

B. "Hardware" means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" and "information" is any communication, representation, information or data and includes all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. Wherefore, I request that the court issue a warrant and order of seizure of the property described above and, further, that the court authorize said property to be examined by qualified personnel employed by the Drug Enforcement Administration; or under direction of the Drug Enforcement Administration, any other law enforcement agency possessing the ability to conduct electronic based forensic or technical analysis, and/or any other private or public sector individual or business possessing the ability to conduct electronic based forensic or technical analysis, on any or all portions of the seized property within a controlled environment.

Pursuant to this warrant, the DEA may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Return of Seized Equipment

If, after inspecting seized equipment, the government determines that the equipment does not contain contraband and the original is no longer necessary to preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking

return will stipulate to a forensic copy's authenticity and accuracy (but not necessarily relevance or admissibility) for evidentiary purposes.

If equipment cannot be returned, agents will make available to the equipment's owner, within a reasonable time period after the execution of the warrant, copies of files that do not contain or constitute contraband; passwords, account information, personally-identifying information of victims; or the fruits or instrumentalities of crime.